



Steps for staying PCI DSS compliant

Visa Account Information Security Guide

October 2009

The guide describes how you can make sure your business does not store sensitive cardholder data



Contents

How to make sure your business does not store Sensitive Cardholder Data	2
Introduction	2
Understanding Cardholder Data	2
Sensitive Authentication Data Explained	4
Track Data	4
Card Verification Value 2 (CVV2)	5
Personal Identification Number (PIN) and PIN Block	5
Understanding Other Types of Cardholder Data	6
Primary Account Number (PAN)	6
Cardholder Name and Expiration Date	7
Service Code	7
Finding Sensitive Authentication Data - Where to Look	8
Detecting Sensitive Authentication Data - How to Look	10
Removing Sensitive Authentication Data	12
Methods by Media	12
Contact Information	13

How to make sure your business does not store Sensitive Cardholder Data

Introduction

Card transactions have become a common way for customers to purchase goods and services at their local retail stores over the Internet and while shopping abroad. To help keep card payments safe and convenient, Visa has helped form an organization called the Payment Card Industry Security Standards Council (PCI SSC).

PCI SSC maintains and supports a number of different security standards, with perhaps the most well known being the PCI Data Security Standard (PCI DSS). This standard details the requirements which all entities that store, process or transmit cardholder data must follow to ensure that cardholder data is kept secure. Two key requirements of the PCI DSS address directly the handling of cardholder data.

These requirements are:

- Do not store¹ sensitive authentication data subsequent to authorization
- Secure non-sensitive authentication data, wherever it is stored

Understanding Cardholder Data

During transaction authorization, the merchant collects data from the payment card and transmits this data to the card issuer. Based on this information the card issuer may either approve or decline the transaction and send the authorization response back to the merchant. This transaction process is illustrated below:

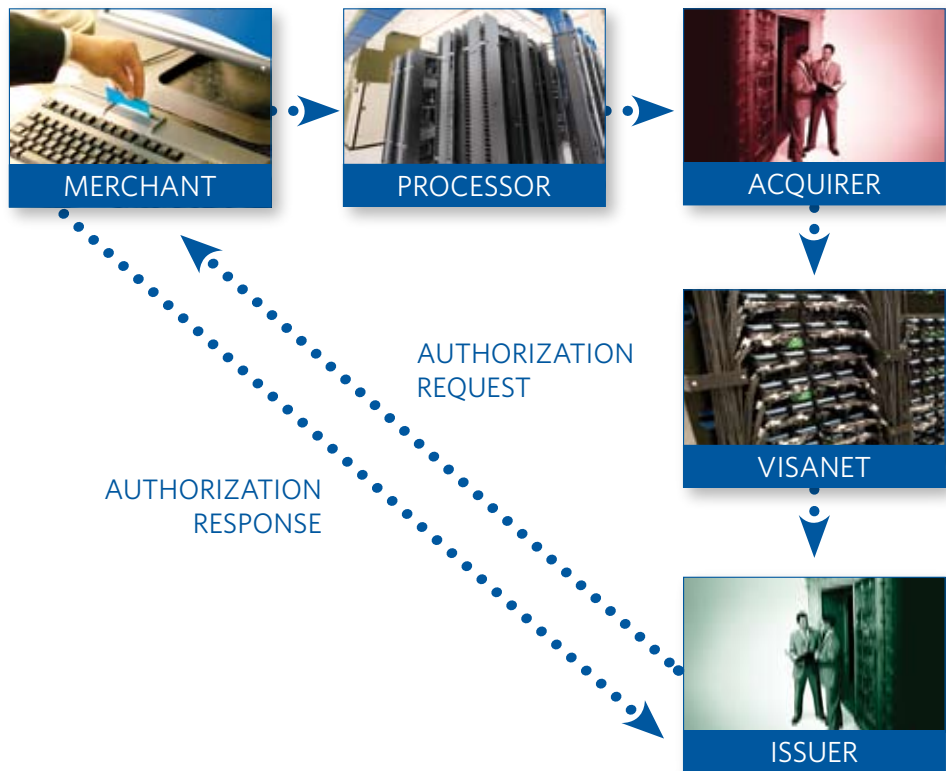


Figure 1

¹Storage is not permitted, even if encrypted.

Transactions are performed using information from the cardholder's payment card and may include other authentication data provided by the customer themselves, such as a signature or a personal identification number (PIN). This information is used by the card issuer to verify and approve transactions, and therefore it is vital that such data is protected.

A representation of a payment card is provided below:



Figure 2

Sensitive cardholder data refers to cardholder data that must not be stored subsequent to transaction authorization. Storage of such data is not permitted under any circumstances, even if the data is encrypted or otherwise protected. There are three types of sensitive cardholder data values, collectively known as 'sensitive authentication data', which are used by the card issuer to confirm the presence of the physical card plastic and/or cardholder at the time of the authorization. The three types of sensitive authentication data are:

- Full contents of the magnetic stripe, also referred to as "Track Data"
- Security code (called a Card Verification Value 2, or CVV2, by Visa)
- PIN or PIN block

In the normal operation of your business there should not be need to store sensitive authentication data subsequent to authorization. Storage of this data decreases the effectiveness of authorization and fraud detection systems in the authorization process and can lead to increased credit card fraud if compromised. Visa does not require that sensitive authorization data be kept subsequent to authorization in fact it is a violation of the PCI DSS requirements and Visa's International Operating Regulations to store such data after authorization.

Sensitive Authentication Data Explained

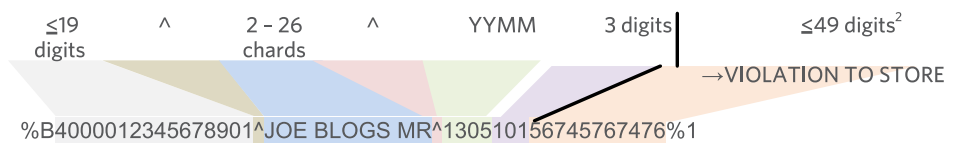
Track Data

Track data is a term used to describe the information that is stored on the magnetic stripe of the payment card. Track data is used by the issuer to confirm the physical presence of the payment card during the transaction. The data is generated by the card issuer and is recorded on the magnetic stripe on the back of the cardholder's plastic, in the chip or both. Each card issuer is able to record discretionary data towards the end of the track.

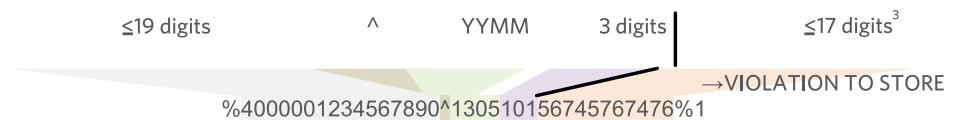
In some instances, it is possible for the track data to be re-constructed using information taken from the magnetic stripe itself or from the chip on the card.

The magnetic stripe can contain up to three tracks of data, each formatted differently, known as Track 1, Track 2 and Track 3. Only Track 1 and Track 2 are used in the payment industry. Track data is defined by international standards and is the same for all card brands.

Track 1



Track 2



The sensitive authentication data can be found towards the end of both Track 1 and Track 2. It is a violation of the Visa International Operating Regulations and the PCI Data Security Standards to store sensitive authentication data subsequent to authorization. Non-sensitive authentication on the track may be stored but must be protected in accordance to the PCI DSS requirements.

² Dependent on the length of other fields in Track 1.
³ Dependent on other fields in Track 2.

Card Verification Value 2 (CVV2)

Visa developed a 3-digit code to help prevent fraud on all manually keyed transactions. The CVV2 code value is different for each payment card even if the cards have the same Primary Account Number (PAN).

The CVV2 resides on the back of the card beside or in the signature panel and is used to confirm the presence of the plastic card in situations where it is not possible to process the magnetic stripe or chip data - i.e. manually keyed transactions including telephone/mail order transactions and Internet transactions.

Each payment brand has a slight difference in the name and location of this code:

- CVV2: Card Verification Value 2 (Visa)
- CVC2: Card Validation Code 2 (MasterCard)
- CID: Card Identification Number (American Express and Discover)
- CAV2: Card Authentication Value 2 (JCB)

Great care needs to be taken with CVV2 since a cardholder may communicate this value to you directly, for example, via your call center or website. Even in these cases, the CVV2 must not be stored post authorization.

Personal Identification Number (PIN) and PIN Block

PIN/PIN block values are used by the card issuer to confirm that the cardholder is present when the purchase is made. A cardholder's PIN value is only known to the cardholder, and the correct value can be verified by the card issuer and its authorized agents.

Cardholder PINs are encrypted into a PIN block for transmission to the merchant's acquirer - this should occur within a secure PIN Entry Device (PED). However, sometimes systems are found that allow for exposure of the customer PIN outside of such secure devices. In both instances, it is not permitted to store the customer PIN block, whether encrypted or not encrypted, after the authorization.

The format for unencrypted PIN blocks is shown below:

Format code (1 digit)	Number of PIN digits (1 hex character)	PIN digits (2 digits)	PIN digits or padding (10 hex characters)	Padding (2 hex characters)
0, 1, 2, 3	0 - 9 or A - C	0 - 9	0 - 9 or A - F	6 - 9 or A - F

Encrypted PIN blocks take the form of 64 bits, or 16 hexadecimal numbers, of random digits. The encrypted PIN block is transmitted in ISO 8583 compliant messages in field 45⁴.

Understanding Other Types of Cardholder Data

As sensitive authentication data, such as the encrypted customer PIN block and the CVV2 value, can be difficult to locate within systems that contain different fields and values, it is often useful to look for areas where other types of cardholder data is stored and then attempt to find sensitive authentication data that may be stored within the same areas.

Primary Account Number (PAN)

The Primary Account Number, also commonly known as the card number, is used to uniquely identify the specific customer account, within a specific card issuer anywhere around the world. Every cardholder has a unique PAN value and this value is found in a number of locations:

- Embossed or printed on the front of the physical plastic
- Digitally record in Track 1 and Track 2 or in the chip
- Databases and paper files
- Transaction records

The PAN may be of any length between 13 and 19 digits, although 16-digit PANs are the most common.

All Personal Account Numbers issued by the payment brands have the following properties, described below.

Starting digits

The digits at the start of the PAN identify the card issuer. The exact method for determining this is not public information.

The following 'rule of thumb' can be used to identify cards issued under the five PCI payment brands.

Visa	4
MasterCard	51 - 55
American Express	34, 37
Discover	6011, 622126 - 622925,644 - 649, 65
JCB	3528 - 3589

Luhn 10 check

The Luhn 10 check formula verifies a number against its check digit (the rightmost digit).

A compliant account number must pass the following test:

1. Counting from the check digit, which is the rightmost digit, and moving left, double the value of every second digit.
2. Sum the digits of the products together with the non-doubled digits from the original number.
3. If the total ends in 0, then the number is valid according to the Luhn formula; otherwise it is not a valid PAN.

As an illustration, if the account number is 49927398716, it will be validated as follows:

1. Double every second digit, from the rightmost:
 $(1 \times 2) = 2$, $(8 \times 2) = 16$, $(3 \times 2) = 6$, $(2 \times 2) = 4$, $(9 \times 2) = 18$
2. Sum all digits (digits in parentheses are the products from Step 1):
 $6 + (2) + 7 + (1 + 6) + 9 + (6) + 7 + (4) + 9 + (1 + 8) + 4 = 70$
3. As the result (70) has a zero on the end and therefore can be divided by ten, the result is a valid PAN value.

Cardholder Name and Expiration Date

Like the PAN, the cardholder name and expiration date may be recorded in a number of places:

- Embossed or printed on the front of the physical plastic
- Digitally record in Track 1 and Track 2 or in the chip
- Databases and paper files
- Call center voice recording
- Transaction records

When printed or embossed, the expiration date is recorded in MM/YY format, but is recorded in track data as YYMM. This date is generated by the card issuer.

Service Code

The service code defines various services, differentiates cards used in international or domestic environments and identifies card restrictions. The service code is digitally recorded in Track 1 and Track 2 or in the chip. It is a 3 decimal digit number and is generated by the card issuer. Common service code values are 101 or 104.

Finding Sensitive Authentication Data — Where to Look

Many businesses believe they are not storing sensitive data because they cannot see it, or because the storage of this data is not a specific part of their business. However, it is important to understand that computer systems and network devices often automatically store data without your knowledge and you must look in all possible storage locations, even if you believe that cardholder data is not deliberately stored.

When looking for sensitive authentication data, it is important to have a good understanding of the types of payments that your company accepts. A merchant that never accepts payments in person would not be handling track or PIN data. A merchant that only accepts payments by swiping a customer card through a POS terminal would not handle CVV2 data.

Therefore, the first step in finding this data is to review the ways in which cardholder data enters and flows through your business. Except for the simplest of merchants, this must be documented, as it will form the cornerstone of your PCI DSS compliance efforts.

The table below indicates common ways sensitive data may enter your business. Once it is in, if not correctly managed, the data may be found anywhere in your business environment!

Business type	Transaction type	Transaction method	Sensitive authentication data ⁵			Cardholder data			
			Track	CVV2	PIN	PAN	Name	Service Code	Expiry
Merchant	Card Present	Magnetic strip or chip	✓	✗	✓	✓	✓	✓	✓
		Manually keyed	✗	✗	✗	✓	✓	✗	✓
	Card Not Present	Manually keyed	✗	✓	✗	✓	✓	✗	✓
		E-commerce	✗	✓	✗	✓	✓	✗	✓
		Recurring transaction	✗	✓	✗	✓	✓	✗	✓
		3rd party file, e.g. outsourced call center	✗	✓	✗	✓	✓	✗	✓
Service Provider	Card not Present	Mail order/ telephone order	✗	✓	✗	✓	✓	✗	✓
		E-commerce	✗	✓	✗	✓	✓	✗	✓
	Others	Others	✓	✓	✓	✓	✓	✓	✓

⁵ Storage of this data (even if encrypted) post authorization is a violation of the data handling requirements.

Other processes that may involve the use of cardholder data include:

- Customer service/transaction dispute
- Merchant settlement
- Customer identification

It is important to take special care when the data passes through computer systems. Modern computer systems often create logs or use 'virtual memory' to ensure smooth system processing - these must also be taken into account while looking for the storage of sensitive data. The scope of your investigation on your computer infrastructure can be significantly reduced (with associated time and money savings) by the implementation of network segmentation (e.g. using VLANs) and firewalls.

However, it should be understood that when looking for the storage of sensitive authentication data you are essentially validating any network segregation that you have put in place - therefore, it is vital that systems that should not be storing, processing or transmitting such data are checked to confirm that this is indeed the case.



Detecting Sensitive Authentication Data —How to Look

The table below describes a number of basic techniques used to find sensitive authentication data. No one way works best in all situations and it is recommended that these methods be adapted and used as befits your environment.

When checking for sensitive authentication data it is important to remember that PCI DSS applies to all systems that store, process or transmit credit card data. This includes hardware systems such as POS devices and ATMs, as well as software systems.

Method	Procedure	Comments
Manually map the flow(s)	<ol style="list-style-type: none"> 1. Manually identify where the data enters your business. 2. Identify (and document) the data flow including all paper-based, voice and system infrastructure, e.g. firewalls, routes, data logs, backups. 3. Investigate each item in the transaction flow, looking for sensitive data. 4. Additionally, if the data is processed on a computer system: <ul style="list-style-type: none"> • Document the computer infrastructure, operating systems and programs used to process the data • Confirm if the programs are on the PA-DSS list and have been implemented in a compliant manner • Confirm if data backups are made and what information is being captured as part of normal business operation 	It is recommended that this be performed for all businesses. Although it may be a labor-intensive task for complex businesses, once it is completed the results are invaluable and will assist you with many of your other PCI DSS compliance tasks.

Method	Procedure	Comments
Scan for known values on computer infrastructure	<ol style="list-style-type: none"> For each of the transaction types used by your business, enter a transaction making note of the values, e.g. PAN, expiry date, CVV2, Track 1, Track 2. Investigate each item in the transaction flow, looking for sensitive authentication data. 	his method is useful for checking for CVV2 and encrypted PIN block values where the data may be difficult to find otherwise.
Scan for known patterns on computer infrastructure	<p>The following data items have known patterns and can be scanned using scanning tools:</p> <ul style="list-style-type: none"> PAN (Luhn 10 check) PAN starting digits Track 1 and Track 2 formats Plaintext PIN block formats 	Common tools and methods are referenced in Appendix I.
Examine database layout for suspicious columns	Review the layout – or schema – of the databases used in your company to see if any columns or entries have headings (such as ‘track data’ or CVV2) that may indicate that sensitive data is being stored.	Do not look for sensitive authentication data only in places where you expect it may be. This data can occur in many different Databases may be used by company-specific systems or may be part of a commercial software package Locations for many different reasons.
Review log and error files	Sensitive authentication data may be stored either deliberately or inadvertently in many different places. Payment software may be designed to store data deliberately for error recovery or communications software logs may be inadvertently storing data.	Do not look for sensitive authentication data only in places where you expect it may be. This data can occur in many different locations for many different reasons.
Confirm error recovery methods for your payment systems	Talk to your payment system vendors and determine how their systems operate if there is an error. Often systems store sensitive authentication data to assist in finalizing payment processing when an error occurs.	When looking for sensitive authentication data it is important to understand the transaction process not only when the payment works, but also what happens when the payment does not work.

Removing Sensitive Authentication Data

The key to achieving PCI DSS compliance is to reduce the number of items that are in scope; that is, to eliminate cardholder data from the business unless it is absolutely required. The less data you have in your business the less you have to control and the easier compliance becomes.

- Where prohibited data is found, take action to eliminate the data as soon as possible and consider changing your business process so the data is no longer retained after authorization
- Introduce procedures so the data is controlled, kept for a minimum time and securely deleted once it's no longer required.

Methods by Media

The following table details common storage locations and suggested actions to assist in compliance.

Media	Actions
Paper/fax	<ul style="list-style-type: none"> • Shred post authorization • Blackout cardholder data with ink
Soft copy images (scanned documents, fax servers)	<ul style="list-style-type: none"> • Alter processes so data is no longer required • Delete post authorization • If possible, electronically black sensitive fields
Call center - call recording	<ul style="list-style-type: none"> • Confirm if CVV2 is being recorded; if it is, consider 'blanking' technology • Encrypt and securely store all call data at a minimum⁶
Computers and computer storage	<ul style="list-style-type: none"> • Use only PA-DSS approved applications • Consult with software developer and confirm if application is PCI DSS compliant and if any special settings are required • Analyze all applications known to handle sensitive data • Scan all storage for PAN and track data, including log and backups
Network equipment	<ul style="list-style-type: none"> • Consult with manufacturer and confirm if device is PCI DSS compliant and if any special settings are required • Analyze all log file for sensitive data
Backups	<ul style="list-style-type: none"> • If backup is pre-authorization, review the purpose of the backup and where possible modify • Encrypt backups

⁶ Storage of sensitive authentication data within voice recordings is acceptable only if there is no commercially feasible method of removing this data, and any such data that is stored is securely encrypted.

Contact Information

For more information on this document or the AIS program, please visit our website at www.visa-asia.com/secured or contact:

Data Security Team

Risk Management
Visa Inc. Asia Pacific
vpssais@visa.com

Or your respective [Visa Country Risk Managers](#):

Ian McKindley

Risk Management
Australia, New Zealand & the Pacific Islands
IMckind@visa.com

Tony Zhu

Risk Management
China
tzhu@visa.com

Murugesh Krishnan

Risk Management
South & Southeast Asia
murugesh@visa.com

Navy Li

Risk Management
China
navyli@visa.com

Abdul Rahim Abdul Rahman

Risk Management
Southeast Asia
aabdulra@visa.com

Vincent Lee

Risk Management
South Korea
vincelee@visa.com

Raveendhrun Anantharaman

Risk Management
South Asia
raveesa@visa.com

Ryoji Ihara

Risk Management
Japan
iryoji@visa.com

Michael Chan

Risk Management
Hong Kong & Taiwan
mikechan@visa.com

Igarashi Kouji

Risk Management
Japan
koigara@visa.com



